PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-150559
(43)Date of publication of application : 23.05.2003

(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 12/14
H04L 9/32

(21)Application number : 2001-352356
(22)Date of filing : 16.11.2001

(71)Applicant : NOGUCHI TOMOKI
(72)Inventor : NOGUCHI TOMOKI
MIYAKE YUJI

(54) KEY SYSTEM FOR PREVENTING ILLICIT USE AND KEEPING SECRECY

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illicit use of an electronic computer system integrated with an electronic computer and a network, to prevent illicit use of information, and to keep secrecy when an electronic recording medium and the computer itself are stolen.
SOLUTION: The illicit use of the electronic computer is prevented by using an optional recording medium as a key. For example, in an enterprise, a system for easily preventing data duplication and browsing can be realized by limiting operation of a client electronic computer to access in a company, or prohibiting operation of the electronic computer itself when the electronic computer is stolen.

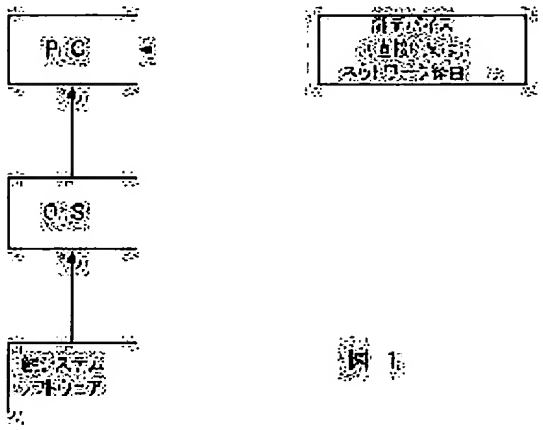

図 1

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００３－１５０５５９

(Ｐ２００３－１５０５５９Ａ)

(43)公開日　平成15年5月23日(2003.5.23)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｇ	5B017
	1/00	３７０		1/00	３７０Ｅ	5B085
	12/14	３２０		12/14	３２０Ｆ	5J104
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｃ	

審査請求　未請求　請求項の数７　ＯＬ　(全５頁)

(21)出願番号　特願2001-352356(P2001-352356)

(22)出願日　平成13年11月16日(2001.11.16)

(71)出願人　501365789
野口　智樹
神奈川県横浜市緑区新治町1025－10

(72)発明者　野口　智樹
横浜市緑区新治町1025－10

(72)発明者　三宅　勇次
横浜市金沢区富岡西1－12－9

(74)代理人　398006604
三宅　勇次

Ｆターム(参考)　5B017 AA03 BB02 BB09
5B085 AA08 AE09 AE11
5J104 AA07 KA01 PA07

(54)【発明の名称】不正使用防止と機密保持のための鍵システム

(57)【要約】
【課題】電子計算機やネットワークで統合された電子計算機の不正な使用防止と電子記録媒体や計算機自体が盗難した場合に、情報の不正使用防止と機密保持を行う。
【解決手段】任意の記録媒体を鍵とすることによって、不正な電子計算機使用を防止する。例えば企業内においてクライアント電子計算機の操作を社内のアクセスに限定、あるいは電子計算機が盗難した場合に電子計算機自体の動作を禁止することにより、不正な電子計算機使用や、データ複製と閲覧を容易に防止するシステムを実現する。

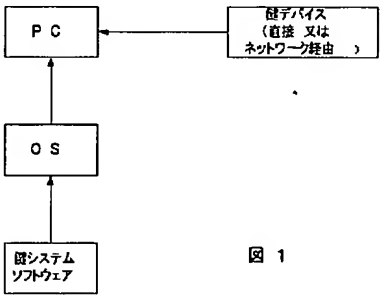

図１

【特許請求の範囲】
【請求項１】電子計算機（以下ＰＣ呼ぶ）と記録媒体（ＭＯ、ＨＤＤ、ＤＶＤ、ＣＤ、フロッピー（登録商標）ディスク、フラッシュメモリ、等）固有の認証鍵情報(ボリュームシリアル番号または製造ロット・シリアル番号またはＰＣのユーザ情報を持つ汎用記録媒体（以下鍵デバイスと呼ぶ）から構成され、鍵デバイスの存在または鍵デバイス内の認証鍵情報が不正に改竄または複製されていないことをＰＣ上で動作するソフトウェアによって認証し、ＰＣの一部または全ての機能制限を解除することが可能な鍵システム。
【請求項２】ＰＣと着脱可能な媒体固有の認証鍵情報を持つ鍵デバイスから構成され、鍵デバイスがＰＣからアクセス可能な状態で鍵デバイス内の認証鍵情報を認証したとき、記録媒体へのアクセスを可能とする鍵システム。
【請求項３】ネットワークで結合されたクライアント・サーバーシステムにおいて、クライアントまたはサーバーに格納された固有の認証鍵情報を、サーバーまたはクライアントのいずれかの認証鍵情報を認証することによって、クライアントＰＣの機能の開始やサーバーへのアクセスを可能としたり、またはクライアントあるいはサーバー機能の制限を解除したりする鍵システム。
【請求項４】上記請求項１～３において認証用鍵情報の認証に、暗号システムを使用または併用する鍵システム。
【請求項５】上記請求項１～４において認証用鍵情報の認証に近距離無線通信（Ｂｌｕｅｔｏｏｔｈ)または遠距離無線通信(携帯電話や携帯端末)のシステムを使用または併用する鍵システム。
【請求項６】上記請求項１～５において鍵デバイスとして近距離無線通信(Ｂｌｕｅｔｏｏｔｈ)または遠距離無線通信(携帯電話や携帯端末)経由によって読み書きできる記録媒体を使用または併用する鍵システム。
【請求項７】上記請求項１～６において、ＰＣまたはサーバー内にある一部または全てのデータを複製先または複製元として、記録媒体を使用または併用する鍵システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】情報処理分野においてＰＣシステムと記録媒体のセキュリティーに関するものである。
【０００２】
【従来の技術】
【０００３】　概要
企業内では古くから電算機システムが実用化され下記の項に示すような保護方法が実施されていたが、企業と言う組織の中でシステムが守られていたため、ネットワークを経由した企業外部からの攻撃や、企業内部であっても可搬性のあるＰＣや記録媒体の盗難に対応するセキュリティー機能が不足していた。
【０００４】　物理的保護
盗難防止のために、ＰＣ筐体に鍵をつけ、机に固定する器具のような物理的保護方法の欠点はＰＣ本体を保護しても、重要なデータが意図せぬ使用者の操作によって複製されてしまうようなデータ漏洩には対応できない。本発明のシステムであれば認証用鍵情報が格納される記録媒体が存在しない限り該当ＰＣ、あるいはデータの内容を閲覧することはできない。
【０００５】　電子的保護
ランダムではあるがアクセス先のサーバーと同期した８桁などの番号が一定間隔で表示されるカード型電子機器においては、使用者はこの番号と一意のパスワードを入力してサーバーへ接続することで、安全性の高い認証が可能となる。この保護方法の欠点はサーバー側にも対応するソフトウェアやハードウェアをインストールする必要があることである。本発明のシステムなら通常サーバー側の設定／対応等は必要なく、最低限ファイル内容の読み出しができるサーバーであれば対応可能である。従って、サーバーに限らず、あらゆる記録媒体（携帯端末、携帯電話、インテリジェント家電機器、ＭＯ、ＨＤＤ、ＤＶＤ、ＣＤ、フロッピーディスク、フラッシュメモリ、等）に適用可能である。
【０００６】　ＯＳによる保護
ＬＡＮ／ＷＡＮで使用されているクライアント／サーバーシステムではパスワードを入力することでシステムへログインが出来る。このシステムではＯＳが管理するパスワードやサーバー上のアプリケーションソフトがＯＳのファイル管理システムに対しディレクトリやファイルに設定するパスワードによる保護法がある。この保護方法の欠点はパスワードが特定のファイルへ記録、あるいはネットワーク上に暗号化されずに流される危険性もあり、情報が他人に漏洩あるいは解読されてしまう可能性が比較的高く、保護としての信頼性は低い。
【０００７】
【発明が解決しようとする課題】ＰＣの不正な使用防止とＰＣ自体または着脱可能な記録媒体が盗難された場合でも当該ＰＣの不正使用防止あるいは機能制限、機密保持、記録媒体に内蔵する情報の漏洩防止を行う。
【０００８】
【課題を解決するための手段】任意の記録媒体（携帯端末、携帯電話、インテリジェント家電機器、ＭＯ、ＨＤＤ、ＤＶＤ、ＣＤ、ＦＤ、フラッシュメモリ等）あるいはネットワーク接続されたサーバー内のディスク内へ認証用鍵情報を格納し適宜認証することによって、不正なＰＣ使用を防止あるいは制限する。例えば企業内においてクライアントＰＣの操作を社内や部署内のアクセスに限定、あるいはＰＣが盗難された場合に、対応する認証用鍵情報を含む記録媒体が存在しないことを検出してＰ

Ｃ自体の動作を禁止あるいは制限することにより、不正なＰＣ使用や、データ複製と閲覧を専用のハードウェアを用いずに低コストで防止するシステムを実現する。

【０００９】ディスク固有情報（ボリュームシリアル番号など）とユーザのパスワード情報やアカウント情報、ユーザが使用するマシンの固有情報などを組み合わせて暗号化の「鍵」としてサーバーへ記録しておくことによって、暗号化された鍵を生成する。

【００１０】ディスク固有情報としてボリュームシリアル番号を用いることで、特定の記録媒体や機器類に限定されない一意の値を汎用的に得ることができる。ボリュームシリアル番号などは、通常はＯＳの用意する各種媒体のフォーマット機能によって、内部的には日時や日時データから生成した一意の番号（マジックナンバー）などから一意といえるＩＤがその都度割り当てられる。従って、通常ＯＳがサポートする記録媒体であれば、携帯端末、携帯電話、インテリジェント家電機器、フロッピーディスク／フラッシュメモリ／ＨＤＤ／ＭＯ／ＣＤ／ＤＶＤ、あるいはネットワーク経由でのサーバー上のディスク領域などの、いかなる記録媒体にも「鍵」としての意味を持たせることが可能となり、同様の手法を適用できる。

【００１１】鍵の認証がとれた場合にのみ、計算機が使用できるように制限するソフトウェアを、使用するＰＣへインストールしておく。例えばＯＳ起動時や、常駐プログラムとして常時実行している時に鍵の認証を行い、鍵の存在が認められない場合やパスワードの不一致などにより認証できない場合はＯＳの処理またはファイルシステムの一部を停止あるいは制限するなどの方法がある。

【００１２】ユーザはＰＣを使用しない場合は、その鍵デバイス付き記録媒体を取り外すことで安全性が確保される。

【００１３】ファイル毎の暗号化についても、この鍵情報をもとにファイル自体を暗号化することが可能。

【００１４】

【発明の実施の形態】

【００１５】記録媒体、を鍵デバイスにする場合には、その鍵デバイスのボリュームシリアル番号と、ユーザのパスワード情報を合成したデータをキーとした暗号化データをファイルとして鍵デバイスへ書き込む。本特許技術を適用したＰＣは、起動時または一定時間間隔または何らかの事象の発生を検出してその鍵を認証し、認証できない場合はそのＰＣ自体の使用が禁止または制限される。制限する機能の種別に応じて、異なる種類の鍵を複数作成することも可能である。

【００１６】サーバー内ディスク（ネットワーク共有ディスク）を鍵にする場合には、サーバー内ディスクのボリュームシリアル番号と、ユーザのパスワード情報を合成したデータをキーとした暗号化データをファイルとして書き込む。本特許技術を適用したＰＣは、起動時または一定時間間隔でその鍵を認証し、認証できない場合はそのＰＣ自体の使用が制限される。制限する機能の種別に応じて、異なる種類の鍵を複数作成することも可能である。

【００１７】請求項２に示す、ネットワークで結合されたクライアント・サーバーシステムにおいて説明する。ネットワークは構内に設置されるＬＡＮまたは遠隔地をインターネット等の通信システムで結ぶ場合がある。第１の操作は、クライアントＰＣをネットワークに接続し、クライアントまたはサーバーからサーバーまたはクライアントＰＣの固有情報(ボリュームシリアル番号または製造ロット・シリアル番号)を読み出し、パスワード情報などと組み合わせて鍵を生成して鍵ファイルへ記録する。第２の操作はクライアントまたはサーバーがサーバー内に格納されている鍵ファイルを認証し、必要であればクライアントＰＣをネッワークへ接続した後、サーバーへ固有情報を送信する。その認証がとれ次第、クライアントＰＣの一部または全ての機能、あるいはサーバーへのアクセスを可能とする。

【００１８】

【実施例】

【００１９】図４に示す実施例は、携帯電話②と接続または内蔵されたデータ保存用のフラッシュメモリ①を鍵デバイスとして用いて、近距離無線通信(Ｂｌｕｅｔｏｏｔｈ)によって、携帯端末③が鍵デバイスの認証をするものである。近距離無線通信はＯＳが標準でサポートしており、鍵システムのソフトウェア(プログラム)から見た場合、携帯電話２と接続または内蔵されたデータ保存用のフラッシュメモリ１は、一般的な携帯端末３に接続されるフラッシュメモリと同様な考え方で操作できるものとする。携帯電話２と接続または内蔵されたデータ保存用のフラッシュメモリ１の鍵デバイスは、許可された使用者のみが胸ポケットなど携帯端末３とは物理的に接続されていない場所に存在し、つまり使用者が携帯端末３から半径１００ｍ以内の近距離無線通信可能な範囲内にいる場合に限り、携帯端末３の使用が許可されるものである。携帯端末３のシステム上で動作する鍵システムの処理プログラムは、携帯電話２との無線接続を常時監視しており、通常はＯＳが管理する近距離無線通信(Ｂｌｕｅｔｏｏｔｈ)関係のイベント(事象)を検出して対応する処理を行うプログラムを記述することによって、携帯電話２が接続されたり、切断されたりする事象に応じて、携帯電話２と接続または内蔵された鍵メディアであるデータ保存用のフラッシュメモリ１の存在を確認して、フラッシュメモリ１のボリュームシリアル番号とを認証し、認証できた場合には、その内部に記録設定された携帯端末３の制限可否情報に応じた携帯端末３の一部または全ての機能制限を解除することが可能となる。携帯端末３の制限可否情報は、鍵デバイスであるフ

5　　6

ラッシュメモリ１の内部に、携帯端末３全体の保護をするのか、使用者の作成したファイルをアクセス禁止するだけの保護をするのか、あるいは画面表示とキーボード操作だけを禁止するのかなどの使用者があらかじめ設定しておいた保護情報である。以上の実施例によって、使用者が無意識のうちに使用する端末の不正使用を、近距離無線通信という非常にシームレスな方法によって防止することができる。

【００２０】鍵デバイス内認証情報ファイル（鍵）の作成処理を下記に箇条書きにて説明する。

1)　PC側で認証情報作成用のソフトウェアを起動

2)　ユーザ名、パスワード、鍵デバイスの場所をユーザが指定

3)　鍵デバイスのボリュームシリアル番号を取得

4)　鍵デバイス内の特定ファイルへ、取得した鍵デバイスのボリュームシリアル番号情報やユーザ情報などを暗号化して保存

5）完了

【００２１】鍵デバイスの認証処理を下記に箇条書きにて説明する。

1）PCの起動時に認証用ソフトウェアを起動しシステムに常駐

2）定期的に鍵デバイスの存在を確認し、存在しない場合は不正使用

と見なしてシステムをプロテクトする。

3）鍵デバイス内の認証情報ファイルを読み出し、暗号化されている情報を復号し、認証情報ファイルに格納されたボリュームシリアル番号と、鍵デバイスのボリュームシリアル番号とが一致するか確認。これが一致しない場合は不正にコピーされた鍵メディアであると判定し、システムをプロテクトする。

【００２２】

【発明の効果】

【００２３】着脱可能な記録媒体や小型ＰＣが盗難された場合、鍵デバイスが無ければ情報として利用できないので、情報の不正利用や漏洩が避けられる。

【００２４】鍵デバイスの装着でシステムの不正使用防止や漏洩が避けられ、サーバー側へ特別なソフトやデバイスを必用としない。

【００２５】認証鍵情報に公開鍵秘密鍵暗号方式を使用すれば、公開性があるインターネットを使用して機密保持と改竄防止をして、鍵システムの認証が出来る。

【００２６】本システムは記録媒体の固有情報の組み合わせだけではなく、ユーザのＩＤやパスワード等の情報を組み合わせることにより、鍵デバイスが盗まれても、鍵デバイスは使用できないので、機密保持と不正使用の防止が出来る。

【図面の簡単な説明】

【図１】図１に、　全体の構成図

【図２】図２に、鍵デバイス内認証情報ファイル（鍵）の作成処理

【図３】図３に、鍵デバイスの認証処理

【図４】図４に　実施例を示す。

【符号の説明】

１----携帯端末

２----ブルートゥース携帯電話

３----フラッシュメモリ

【図１】

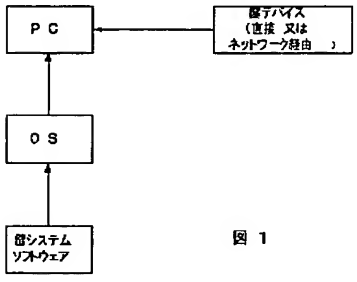

図 1

【図２】

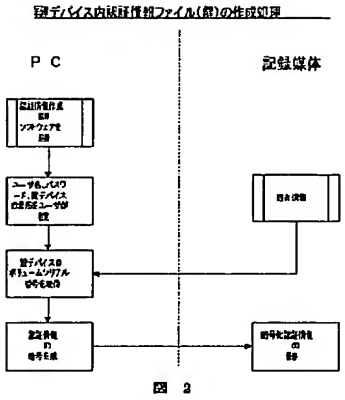

図 2

【図３】

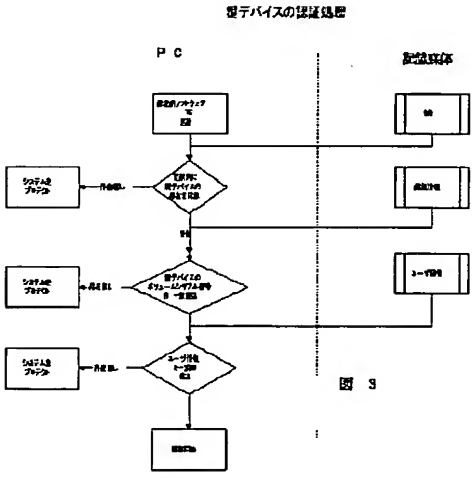

図 3

【図４】

図 4